UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/764,513	01/27/2004	Hidenori Nanki	56937-108	9962

7590 12/14/2007

McDERMOTT, WILL & EMERY
600 13th Street, N.W.
Washington, DC 20005-3096

EXAMINER	
KROFCHECK, MICHAEL C	
ART UNIT	PAPER NUMBER
2186	

MAIL DATE	DELIVERY MODE
12/14/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/764,513	NANKI ET AL.	
	Examiner	Art Unit	
	Michael Krofcheck	2186	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 October 2007*.

2a)☒ This action is FINAL. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2 and 6-21* is/are rejected.

7)☒ Claim(s) *3-5* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 January 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to the amendments filed on 10/3/2007.

2. The title, abstract, specification, and claims 1-10 have been amended.

3. New claims 11-21 have been added and examined.

4. The objections/rejections not restated herein have been withdrawn.

Claim Warnings

5. Applicant is advised that should claims 16-17 be found allowable, claims 20-21 will be objected to under 37 CFR 1.75 as being a substantial duplicate thereof. Then two claims in an application are duplicates or else are so close in content That they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 12-21 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

8. Claims 12-21 recite the limitations "the mode" in each claim. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

11. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of

35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

12. Claims 1 and 12-13 are rejected under 35 U.S.C. 103(a) over Abraham et al., US patent 5237616, and Guttag et al., US patent 4590552.

13. With respect to claim 1, Abraham teaches of an information processing apparatus for accessing memory spaces including a user memory space and a secure memory space (fig. 1; item 105, 109), comprising: a general purpose register used for an arithmetic operation of a CPU and having a function of receiving, delivering and storing data, the general purpose register having a data unit (fig. 1; column 2, lines 45-48; the Intel 80C186 processor inherently contains general purpose registers used for arithmetic operation and I/O operations that have data units. Intel's "80C186EA/80C188EA Microprocessor User's Manual" provides support for this in sections 2.1, 2.1.3 on pages 2-1, 2-4 to 2-5);

a secure information unit adapted to be set to a state not requiring security in a case that the data is transferred from the user memory space to the data unit of the general purpose register, and adapted to be set to a state requiring security in a case that the data is transferred from the secure memory space to the data unit of the general purpose register (fig. 2, column 3, lines 35-50);

a data control unit having a function of determining whether a value of the secure information unit is in the state requiring security or the state not requiring security when the data of the general purpose register is written in the user memory space, thereby determining whether a data transfer to the user memory space is prohibited or not (fig. 1; item 107, column 2, lines 57-67); and

an address control unit having a function of determining which of the user memory space and the secure memory space is indicated by an address information, and selecting the value of the secure information unit (fig. 1; item 210, column 3, lines 10-12).

Abraham fails to explicitly teach of the secure information unit being included in the general purpose registers. However, Guttag teaches of a security bit register indicating a state of protected or non-protected status of memory (column 2, lines 3-28; claim 1, column 8, lines 56-60).

It would have been obvious to one of ordinary skill in the art having the teachings of Abraham and Guttag at the time of the invention to store the state of Abraham in a register as taught in Guttag. Their motivation would have been to provide high speed access to the security state.

14. With respect to claim 12, Guttag teaches of wherein the data control unit determines whether the data transfer to the user memory space is prohibited or not irrespective of the mode associated with a CPU (column 2, lines 3-54).

15. With respect to claim 13, Abraham teaches of wherein the mode associated with the CPU includes a privileged mode or an unprivileged mode (column 2, lines 57-61).

16. Claims 2 and 11 rejected under 35 U.S.C. 103(a) as being unpatentable over Abraham and Guttag as applied to claim 1 in view of Banno et al., US patent 5680581.

17. With respect to claim 2, Abraham teaches of a user program arranged in the user memory space; and a secure program arranged in the secure memory space (column 1, lines 54-63);

an instruction buffer used by the CPU to fetch the instruction code and having a function of storing therein the instruction code input from the data control unit, (the 80C186 contains an instruction queue which holds the instructions until used by the CPU, "80C186EA/80C188EA Microprocessor User's Manual" provides support for this in sections 2.1.1, pages 2-2 to 2-3);

wherein, when the data control unit executes the data transfer from the data unit of the general purpose register to the memory spaces in compliance with a transfer instruction, the data transfer to the user memory space is prohibited, if the secure information unit indicates the state requiring security (column 2, lines 50-67).

Abraham fails to explicitly teach of an instruction fetch address control unit having a function of determining which of the user memory space and the secure memory space is indicated by the address information.

However, Banno teaches of an instruction fetch address control unit having a function of determining which of the user memory space and the secure memory space is indicated by the address information when storing an instruction code input from the data control unit (column 3, lines 43-51), and

a function of notifying the data control unit which of the user program and the secure program is under execution (column 2, lines 5-9);

wherein, when the data control unit executes the data transfer from the data unit of the general purpose register to the memory spaces in compliance with a transfer instruction, the data transfer to the user memory space is prohibited, if the instruction fetch address control unit determines that the instruction code is fetched from the user memory space and the value of the secure information unit indicates the state requiring security (column 3, lines 51-56, column 2, lines 5-9).

It would have been obvious to one of ordinary skill in the art having the teachings of Abraham and Banno at the time of the invention to prohibit reading out from the internal memory to an external memory in Abraham as taught in Banno. Their motivation would have been to prevent a third party from gaining knowledge of the internal program (column 1, lines 20-24).

18. With respect to claim 11, Abraham teaches of wherein the user program is accessible mainly by a user, and the secure program is accessible mainly by a developer and contents of the secure program is not disclosed to the user (column 1, lines 54-63).

19. Claim 6 rejected under 35 U.S.C. 103(a) as being unpatentable over Abraham, Ishimoto, US patent 6101586 and Koizumi, US patent 5414864.

20. With respect to claim 6, Abraham teaches of an information processing apparatus for accessing memory spaces including a user memory space and a secure memory space (fig. 1; item 105, 109), comprising: a secure information generating unit for determining which of the user memory space and the secure memory space is indicated by address information (column 2, lines 57-67, as

data is restricted from accessing a memory in either circumstance, it is abundantly clear to one of ordinary skill in the art that there is something that determines which memory the access is directed to through its address), and

delivering data with secure information into a general purpose register with secure information having a function of receiving and holding the data with secure information (fig. 1; column 2, lines 45-48; the Intel 80C186 processor inherently contains general purpose registers used for arithmetic operation and I/O operation. Intel's "80C186EA/80C188EA Microprocessor User's Manual" provides support for this in sections 2.1, 2.1.3 on pages 2-1, 2-4 to 2-5);

a built-in memory space for receiving and holding the data with secure information from the general purpose register and delivering the data with secure information held to the general purpose register (fig. 1; item 105, 109); and

a data output control unit having a function of controlling a data transfer to an external space by using the secure information (column 2, lines 57-67);

wherein the data output control unit performs a control operation to determine whether the data transfer to the external space is prohibited or not by a value of the secure information (column 2, lines 57-67; column 3, lines 10-12).

Abraham fails to explicitly teach of the built-in memory space being a RAM. However, Ishimoto teaches of the built-in memory space being a RAM (column 11, lines 46-49).

Abraham fails to explicitly teach of a value of the secure information being set in the general purpose register. However, Koizumi teaches of a status value being set in the general purpose register (column 2, lines 36-42).

It would have been obvious to one of ordinary skill in the art having the teachings of Abraham and Ishimoto at the time of the invention to use RAM as the unprivileged memory in Abraham as taught in Ishimoto, since RAM is the most commonly available and most versatile type of memory.

It would have been obvious to one of ordinary skill in the art having the teachings of Abraham, Ishimoto, and Koizumi at the time of the invention to indicate the privileged and unprivileged states in the GPR of Abraham as taught in Koizumi so the status is directly accessible by the processor.

21. Claims 14-15 rejected under 35 U.S.C. 103(a) as being unpatentable over Abraham, Ishimoto, and Koizumi as applied to claim 6 above, and in further view of Guttag.

22. With respect to claim 14, Guttag teaches of wherein the data control unit determines whether the data transfer to the user memory space is prohibited or not irrespective of the mode associated with a CPU (column 2, lines 3-54).

It would have been obvious to one of ordinary skill in the art having the teachings of Abraham, Ishimoto, Koizumi, and Guttag at the time of the invention to determine the allowability of data transfer independently of the CPU in the combination of Abraham, Ishimoto, Koizumi as taught in Guttag so that the protection of software is extended against numerous external peripheral devices (Guttag, column 1, lines 65-68).

23. With respect to claim 15, Abraham teaches of wherein the mode associated with the CPU includes a privileged mode or an unprivileged mode (column 2, lines 57-61).

24. Claim 9 rejected under 35 U.S.C. 103(a) as being unpatentable over Abraham, Ishimoto, Koizumi and Banno.

25. With respect to claim 9, the combination of Abraham, Ishimoto, Koizumi teach of the limitations cited above with respect to claim 6.

Abraham fails to explicitly teach of a direct memory access unit with secure information having a function of holding the secure information. However, Banno teaches of a computer system including a direct memory access controller (column 1, lines 11-15).

It would have been obvious to one of ordinary skill in the art having the teachings of Abraham, Ishimoto, Koizumi and Banno at the time of the invention to incorporate the DMA controller of Banno into the combination of Abraham, Ishimoto, Koizumi. Their motivation would have been to allow for data transfer to take place without the processor controlling it, thus creating more available processing time.

26. Claims 18-19 rejected under 35 U.S.C. 103(a) as being unpatentable over Abraham, Ishimoto, Koizumi and Banno as applied to claim 9 above, and in further view of Guttag.

27. With respect to claim 18, Guttag teaches of wherein the data control unit determines whether the data transfer to the user memory space is prohibited or not irrespective of the mode associated with a CPU (column 2, lines 3-54).

It would have been obvious to one of ordinary skill in the art having the teachings of Abraham, Ishimoto, Koizumi, Banno, and Guttag at the time of the

invention to determine the allowability of data transfer independently of the CPU in the combination of Abraham, Ishimoto, Koizumi and Banno as taught in Guttag so that the protection of software is extended against numerous external peripheral devices (Guttag, column 1, lines 65-68).

28. With respect to claim 19, Abraham teaches of wherein the mode associated with the CPU includes a privileged mode or an unprivileged mode (column 2, lines 57-61).

29. Claims 7-8, 10 rejected under 35 U.S.C. 103(a) as being unpatentable over Abraham, Ishimoto, Koizumi, Banno, and Garney, US patent 5386552.

30. With respect to claim 7, the combination of Abraham, Ishimoto, and Koizumi teach of the limitations cited above with respect to claim 6.

Abraham fails to explicitly teach of delivering an instruction with secure information into an instruction decoder with secure information having a function of determining which of the user memory space and the secure memory space is associated with the instruction under execution.

However, Banno teaches of delivering an instruction with secure information into an instruction decoder with secure information having a function of determining which of the user memory space and the secure memory space is associated with the instruction under execution (column 3, lines 44-51);

Abraham fails to explicitly teach of an interrupt saved information unit with secure information having a function of adding, upon generation of an interrupt process, the secure information of the instruction decoder to data saved in a stack area of the built-in RAM space.

However, Garney teaches of a built-in RAM space with secure information for receiving and holding the data with secure information from the general purpose register and delivering the data with secure information held to the general purpose register (column 1, lines 17-40; in the combination in an interrupt processing or context switch, the GPR from the processor of Abraham are saved in the stack of Garney);

an interrupt saved information unit with secure information having a function of adding, upon generation of an interrupt process, the secure information of the instruction decoder to data saved in a stack area of the built-in RAM space (column 1, lines 17-40).

It would have been obvious to one of ordinary skill in the art having the teachings of Abraham, Ishimoto, Koizumi, and Banno at the time of the invention to identify the memory associated with the requested instruction in the combination of Abraham, Ishimoto, and Koizumi as taught in Banno. Their motivation would have been to prevent a third party from gaining knowledge of the internal program (column 1, lines 20-24).

It would have been obvious to one of ordinary skill in the art having the teachings of Abraham, Ishimoto, Koizumi, Banno, and Garney at the time of the invention store the processor context upon an interrupt occurrence in the combination as taught in Garney. Their motivation would have been to enable multitasking, thus increasing the efficiency of the processor.

31. Claims 16-17, 20-21 rejected under 35 U.S.C. 103(a) as being unpatentable over Abraham, Ishimoto, Koizumi, Banno, and Garney as applied to claim 7 above, and in further view of Guttag.

32. With respect to claims 16 and 20, Guttag teaches of wherein the data control unit determines whether the data transfer to the user memory space is prohibited or not irrespective of the mode associated with a CPU (column 2, lines 3-54).

It would have been obvious to one of ordinary skill in the art having the teachings of Abraham, Ishimoto, Koizumi, Banno, Garney, and Guttag at the time of the invention to determine the allowability of data transfer independently of the CPU in the combination of Abraham, Ishimoto, Koizumi, Banno, and Garney as taught in Guttag so that the protection of software is extended against numerous external peripheral devices (Guttag, column 1, lines 65-68).

33. With respect to claims 17 and 21, Abraham teaches of wherein the mode associated with the CPU includes a privileged mode or an unprivileged mode (column 2, lines 57-61).

34. With respect to claim 8, the combination of Abraham, Ishimoto, Koizumi, Banno, Garney teach of the limitation cited above with respect to claim 7.

Garney also teaches of a stack pointer for defining a part of the built-in RAM space as the stack area (column 1, lines 25-29; it is abundantly clear to one of ordinary skill in the art that a stack comprises stack pointers which define the stack); and

a saved information rewrite control unit for controlling a rewrite operation in the stack area of the built-in RAM space (column 1, lines 25-29; it is abundantly clear to one of ordinary skill in the art that since data is written to and from the stack, there must be something that controls this);

The combination of Abraham, Ishimoto, Koizumi, Banno, Garney teaches of wherein the saved information rewrite control unit prohibits the rewrite operation if the instruction of the instruction decoder is associated with the user memory space and intended to rewrite the stack area of the built-in RAM space (since in the combination, writing something that does not originate within the internal memory to an internal memory is inhibited by the protection circuit of Banno, writing state information involving instruction not from the internal memory into an internal RAM stack would not be allowed).

35. With respect to claim 10, the combination of Abraham, Ishimoto, Koizumi, Banno, Garney teach of the limitation cited above with respect to claim 7.

Banno teaches of an operating unit with secure information having a function of reflecting the secure information of the instruction decoder in an arithmetic operation executed in accordance with the instruction decoded by the instruction decoder (column 1, lines 55-65, column 3, lines 44-56).

Allowable Subject Matter

36. Claims 3-5 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

37. The following is a statement of reasons for the indication of allowable subject matter:

a. With respect to claim 3, the prior art does not teach of the secure information unit of the general purpose registers storing the result of the arithmetic operation being set in an invalid security state when the value of the secure information unit of one of the general purpose registers requires security in combination with the other limitations as set forth in the claim.

b. With respect to claim 4, the prior art does not teach of a status register keeping the value of each flag unchanged when the secure information unit of one of the general purpose registers requires security in combination with the other limitations as set forth in the claim.

c. With respect to claim 5, the prior art does not teach of a debug key that when read out by the CPU through the secure IO space when the developer debugs the secure program with the user system, halts the address determining function of the instruction fetch address control unit in combination with the other limitations as set forth in the claim.

Response to Arguments

38. Applicant's arguments filed 10/3/2007 have been fully considered but they are not persuasive.

39. Applicant argues with respect to claim 1, that Abraham fails to teach of a secure information unit included in the general purpose register and adapted to

be set to a state not requiring security in a case that the data is transferred from the user memory space to the data unit of the general purpose register, and adapted to be set to a state requiring security in a case that the data is transferred from the secure memory space to the data unit of the general purpose register; a data control unit having a function of determining whether a value of the secure information unit is in the state requiring security or the state not requiring security when the data of the general purpose register is written in the user memory space, thereby determining whether a data transfer to the user memory space is prohibited or not; specifically that Abraham doesn't teach of the **secure information unit included in the general register determining the data transfer area**. The examiner disagrees.

As clamed, claim one does not disclose what unit actually determines the data transfer areas (the security state). The secure information unit stores an indication of the current security state (security required, or no security required), and the data control unit reads that security state to determine how to act on it. There is nothing claimed that indicates what determines the security state/transfer areas in claim 1.

40. With respect to claims 6-10, applicant specifically argues that Abraham does not teach or suggest assigning to the data itself a particular mode and storing the data with the particular mode and that the other references don't remedy this short coming of Abraham. The examiner disagrees with this basis for argument.

As claimed, the data is indicated as, "data with secure information". There is no explanation as to what this secure information is, what it represents, or how it is associated with the claimed data. It is the examiner's interpretation that since the addresses in Abraham are used to determine the privileged or unprivileged states that the address associated with the data is the "secure information". The examiner suggests the applicant clarify what the secure information is and how it is linked to the claimed data.

Conclusion

41. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

42. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

43. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Krofcheck whose telephone number is 571-272-8193. The examiner can normally be reached on Monday - Friday.

44. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Matt Kim can be reached on 571-272-4182. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

45. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Michael Krofcheck

MATTHEW KIM
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100